



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002064561 A**(43) Date of publication of application: **28.02.02**

(51) Int. Cl. **H04L 12/56**
H04L 12/24
H04L 12/26

(21) Application number: **2000255739**(22) Date of filing: **22.08.00**(71) Applicant: **HITACHI LTD**

(72) Inventor: **SUZUKI MASARO**
SHIINA TEI
TAIRA MASANORI

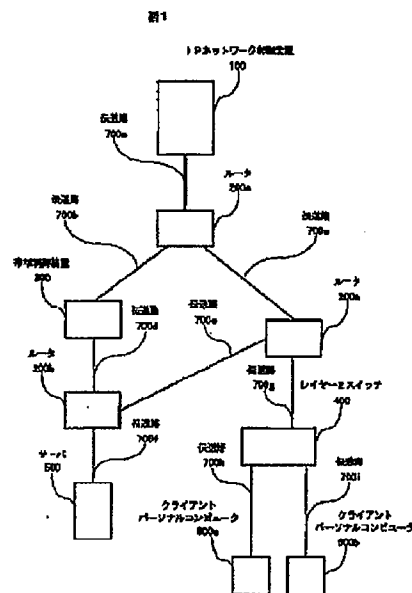
(54) **NETWORK CONTROL APPARATUS AND
 NETWORK CONTROL METHOD**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a network control apparatus that selects optimum network control information in response to an operating state of a network and transmits the selected information to a device connected to the network.

SOLUTION: Information with respect to the operating state of the network is collected from devices connected to the network, and control contents to control the network and control information defining executing conditions of the control contents are selected on the basis of the collected operating state of the network, and the selected control information is distributed to the devices connected to the network to control them.

COPYRIGHT: (C)2002,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-64561
(P2002-64561A)

(43) 公開日 平成14年2月28日 (2002.2.28)

(51) Int.Cl. ⁷	識別記号	F I	データベース*(参考)
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 Z 5 K 0 3 0
12/24		11/08	
12/26			

審査請求 未請求 請求項の数 6 O L (全 15 頁)

(21) 出願番号 特願2000-255739(P2000-255739)

(22) 出願日 平成12年8月22日 (2000.8.22)

(71) 出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(72) 発明者 鈴木 政朗
神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所社会・ネットワークシステム事業部内

(72) 発明者 椎名 倅
神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所社会・ネットワークシステム事業部内

(74) 代理人 100075096
弁理士 作田 康夫

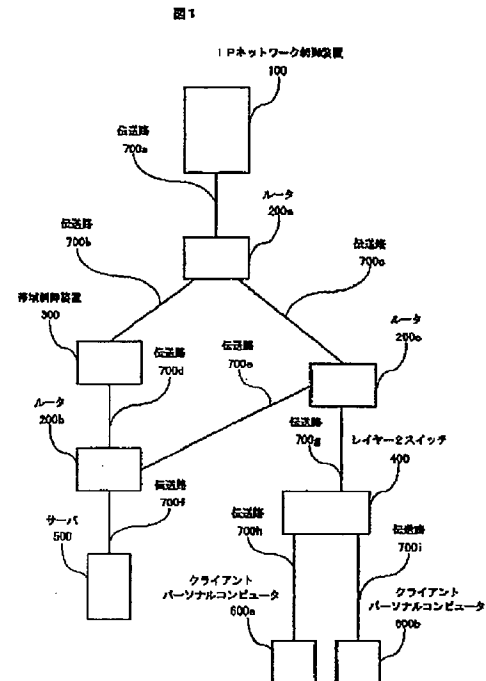
最終頁に続く

(54) 【発明の名称】 ネットワーク制御装置及びネットワーク制御方法

(57) 【要約】

【課題】 ネットワークの使用状況に応じた最適なネットワーク制御情報を選択し、送付する。

【解決手段】 ネットワークに接続された装置からネットワークの使用状況に関する情報を収集し、収集したネットワークの使用状況に基づいてネットワークを制御するための制御内容とその制御内容の実施条件を定義した制御情報を選択し、選択した制御情報をネットワークに接続された装置に配布して制御を行う。



【特許請求の範囲】

【請求項1】 ネットワークに接続された装置を制御するネットワーク制御装置であって、前記ネットワークに接続された装置からネットワークの使用状況に関する情報を収集するネットワーク情報管理部と、ネットワークを制御するための制御内容と該制御内容の実施条件を定義した制御情報を蓄積するネットワーク制御情報蓄積部とを有し、前記収集したネットワークの使用状況に基づいて前記制

御情報蓄積部から制御情報を選択して前記ネットワークに接続された装置に配布することによりネットワークの制御を行うことを特徴とするネットワーク制御装置。

【請求項2】 ネットワークに接続された装置を制御するネットワーク制御装置であって、前記ネットワークに接続された装置からネットワーク内のトラヒックに関する情報を収集し、前記収集したトラヒック情報を定量化するトラヒック管理部と、ネットワークを制御するための制御内容と該制御内容の実施条件を定義したネットワーク制御情報を蓄積したネ

ットワーク制御情報蓄積部と、該定量化した結果に基づいて前記ネットワーク制御情報蓄積部に蓄積されているネットワーク制御情報を検索し、前記ネットワークに接続された装置に配布するネットワーク制御部とを有することを特徴とするネットワーク制御装置。

【請求項3】 前記トラヒック管理部は、前記収集したトラヒックに関する情報から評価パラメータを抽出し、前記評価パラメータをもとにネットワークの使用状況をメンバシップ関数を用いて定量化し、該定量化した値に

基づいて前記ネットワークに接続された機器にネットワーク制御情報の送付の可否を判断し、要の場合には前記ネットワーク制御部にネットワーク制御情報を検索して配布するよう要求することを特徴とする前記請求項1または2に記載のネットワーク制御装置。

【請求項4】 ネットワークに接続された装置を制御するネットワーク制御方法であって、前記ネットワークに接続された装置からネットワークの使用状況に関する情報を収集し、前記収集したネットワークの使用状況に基づいてネットワークを制御するための制御内容と該制御内容の実施条件を定義した制御情報を選択し、該選択した制御情報を前記ネットワークに接続された装置に配布して制御を行うことを特徴とするネットワーク制御方法。

【請求項5】 ネットワークに接続された装置を制御するネットワーク制御方法であって、前記ネットワークに接続された装置からネットワーク内のトラヒックに関する情報を収集し、収集したトラヒック情報を定量化し、該定量化した結果に基づいてネットワークを制御するための制御内容と該制御内容の実施条件を定義したネット

ワーク制御情報を検索し、前記ネットワークに接続された装置に配布することを特徴とするネットワーク制御方法。

【請求項6】 前記収集したトラヒックに関する情報から評価パラメータを抽出し、前記評価パラメータをもとにネットワークの使用状況をメンバシップ関数を用いて定量化し、該定量化した値に基づいて前記ネットワークに接続された機器にネットワーク制御情報の送付の可否を判断し、要の場合には前記ネットワーク制御情報を検索して配布することを特徴とする前記請求項4または5に記載のネットワーク制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、コンピュータネットワークを介した機器の制御に関し、特に、インターネット・プロトコル (Internet Protocol 以下、IP) ネットワークにおいてネットワークの状況に応じた制御を行うIPネットワーク制御装置およびIPネットワーク制御方法に関する。

【0002】

【従来の技術】 近年、インターネット基盤が普及し、インターネットを用いたデータ通信コストが安価になりはじめてきたため、多くのユーザや、各種のトラヒックがIPネットワークに集約される傾向にある。今後は、通話音声もIPネットワークに集約される傾向である。このように各種トラヒックを1つのIPネットワークに相乗りさせると、バースト性の高いFTP (File Transfer Protocol) やHTTP (HyperText Transfer Protocol) などのトラヒックが、遅延やゆらぎに弱いホスト・データや通話音声などの転送を妨げてしまう。また、トラヒックの性質も、機密性の高いトラヒックから一般のトラヒックまで様々である。そのため、ネットワークのセキュリティを確保する方法が複雑になる。

【0003】 以上のような問題を抱えるIPネットワークにおいて、ネットワーク上を流れる各トラヒックの“交通整理”を実現するためにポリシー・ベース・ネットワークが登場した。ポリシー・ベース・ネットワークとは、アプリケーションやユーザ単位に、パケット転送の優先度・使用帯域制御・セキュリティなどのポリシー情報を策定し、IPネットワーク内のすべての各種IPネットワーク機器はそのポリシー情報に従うことで、IPネットワーク全体でトラヒックの制御を行う仕組みである。ポリシー情報は、ポリシー制御を実施する“条件” (たとえば、「通話音声トラヒックが流れたら」「優先度の高いトラヒックが流れたら」など) と、パケット処理方法 (「64 kbit/sを確保する」「最優先で転送する」など) が定義されている。このようなポリシー情報に基づいたネットワーク制御に関する技術としては、例えば特開2000-83048号公報に記載されたようなものがある。

【0004】ポリシー・ベース・ネットワークにおいては、IPネットワーク機器の設定を一元化できるため、ネットワーク全体のQoS (Quality Of Service) やセキュリティを確保しつつ、ネットワーク管理者の負担を抑えられる。

【0005】

【発明が解決しようとする課題】上記従来の技術においては、ポリシー情報は、ネットワーク管理者が経験に基づき策定し配布するか、またはリモート・ネットワーク・モニタリング (RemoteNetwork Monitoring 以下、RMON) プローブや、管理情報ベース (Management Information Base 以下、MIB) 等で収集されたパケット数や帯域使用率等のトラヒック情報からIPネットワークの使用状況を予測して策定されたものであった。(例えば、「通話音声トラヒックが流れてきたら、64kb/sで転送」「午後6時から午後1時まで、A宛のトラヒックの為に帯域を50%確保」というように策定。)しかし、完全なポリシーを策定し、IPネットワークをポリシー制御するためには、ユーザごと、アプリケーションごと、時間ごと、インタフェースごと等、きめ細かくトラヒックを分析し、IPネットワークの使用状況に応じた最適なポリシー情報を、最適な契機に配布する必要がある。

【0006】本発明は、上記の事情に鑑みてなされたものであり、ネットワーク管理者が任意に決めるようなしきい値を用いて「何Kbps以上はトラヒックが多い」「何%以下は帯域が不足」と判断するのではなく、ネットワークの使用状況に応じたポリシー制御が実施できるネットワーク制御装置およびネットワーク制御方法を提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するため、本発明は、ネットワークに接続された装置からネットワーク内のトラヒックに関する情報を収集し収集したトラヒック情報を定量化するトラヒック管理部と、ネットワークを制御するための制御内容とその制御内容の実施条件を定義したネットワーク制御情報を蓄積したネットワーク制御情報蓄積部と、定量化した結果に基づいてネットワーク制御情報蓄積部に蓄積されているネットワーク制御情報を検索し、ネットワークに接続された装置に配布するネットワーク制御部を有するようにしたものである。

【0008】また、トラヒック管理部は、収集したトラヒックに関する情報から評価パラメータを抽出し、評価パラメータをもとにネットワークの使用状況をメンバシップ関数を用いて定量化し、定量化した値に基づいてネットワークに接続された機器にネットワーク制御情報の送付の可否を判断し、要の場合にはネットワーク制御部にネットワーク制御情報を検索して配布するよう要求するようにした。

【0009】また、本発明のネットワーク制御方法は、ネットワークに接続された装置からネットワークの使用状況に関する情報を収集し、収集したネットワークの使用状況に基づいてネットワークを制御するための制御内容とその制御内容の実施条件を定義した制御情報を選択し、選択した制御情報をネットワークに接続された装置に配布して制御を行うようにした。

【0010】

【発明の実施の形態】以下、本発明を実施の形態を、図面を用いて説明する。図1は、本発明を適用したIPネットワークの構成の一例を示す図である。図1に示すIPネットワークは、IPネットワーク制御装置(100)と、複数のルータ(200a~200c)と、帯域制御装置(300)と、レイヤー2スイッチ(400)と、サーバ(500)と、複数のパーソナルコンピュータ(600a~600b)と、伝送路(700a~700i)とから構成される。

【0011】本発明においては、IPネットワーク制御装置(100)は、ルータ(200a~200c)や、帯域制御装置(300)や、レイヤー2スイッチ(400)から収集したトラヒックに関する情報を処理し、最適なポリシー情報を、最適な契機にルータ(200a~200c)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に伝送路(700a~700i)を介して配布する。ルータ(200a~200c)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、その配布されたポリシー情報にもとづいてQoSやセキュリティの設定を変更する。

【0012】次に、IPネットワーク制御装置について説明する。図2は、IPネットワーク制御装置の構成を示す図である。本実施の形態において、IPネットワーク制御装置(100)は、ポリシー情報蓄積部(101)と、ポリシー制御部(102)と、トラヒック管理部(103)と、トラヒック情報解析機構(104)と、トラヒック情報処理機構(105)と、トラヒック情報蓄積機構(106)と、外部インタフェース(107)とから構成される。

【0013】ポリシー情報蓄積部(101)は、外部インタフェース(107)から入力されたポリシー情報を蓄積し、ポリシー制御部(102)は、トラヒック管理部(103)で処理されたトラヒック情報にもとづいてポリシー情報をポリシー情報蓄積部(101)から検索し、外部インタフェース(107)を介して、複数のルータ(200a~200c)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に配布する。トラヒック管理部(103)は、トラヒック情報解析機構(104)と、トラヒック情報処理機構(105)と、トラヒック情報蓄積機構(106)とから構成される。トラヒック情報解析機構(104)は、複数のルータ(200a~200c)や、帯域制御装置(300)や、レイヤー2スイッチ(400)から受信したトラヒックに関する情報を解析し、各インタフェースで送受信されたIPパケットのオクテット数や、各インタフェースの帯域使用率や、各インタフェースで廃棄されたIPパケット数等の情報を収集し、また、ポリシー制

御部(102)からIPネットワークのトラヒックに関する情報収集の要求を受けた場合は、複数のルータ(200a~200c)や、帯域制御装置(300)や、レイヤー2スイッチ(400)にトラヒック情報収集を行うためのパケットを送受信する機能を有する。

【0014】トラヒック情報蓄積機構(106)は、収集されたIPネットワーク内のトラヒックに関する情報を解析し、解析結果を日単位のトラヒック特性を示す日別トラヒック情報や、時間単位のトラヒック特性を示す時間別トラヒック情報として蓄積する。トラヒック解析機構(104)は、蓄積されたIPネットワーク内のトラヒックに関する情報をもとに、現在のネットワーク内のトラヒック状況を判断したり、今後のネットワーク内のトラヒック状況を予見し、ルータ(200a~200c)や、帯域制御装置(300)や、レイヤー2スイッチ(400)にポリシー情報を配布すべきか否かを判定し、配布すべきであれば外部インタフェース(107)を介し、ポリシー制御部(102)に対し、ポリシー情報配布要求を出す。

【0015】ネットワーク管理者から投入された、詳細まで定義されていないポリシー・サマリー情報を受信した場合には、ポリシー制御部(102)は、トラヒック管理部(103)からIPネットワークのトラヒックに関する情報を収集し、ポリシー情報蓄積部(106)からポリシー情報を検索し、ルータ(200a~200c)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に検索したポリシー情報を配布する。

【0016】次に、本発明のポリシー情報配布処理について図3ないし図9を用いて説明する。まず、本発明のポリシー情報配布処理の大まかな流れを説明する。図3は、ポリシー情報配布処理の概要を示す図である。ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、定期的又はIPネットワーク制御装置(100)からの要求があった場合に、RMONで収集したトラヒックの統計情報や、MIB情報などの、IPネットワークのトラヒックに関する情報を、IPネットワーク制御装置(100)に送信する(3e)(3f)(3g)。

【0017】IPネットワーク制御装置(100)のトラヒック管理部(103)は、外部インタフェース(107)を介してIPネットワークのトラヒックに関する情報を受信する(3d)。

【0018】トラヒック管理部(103)のトラヒック情報処理機構(105)は、受信したトラヒックに関する情報を解析し、各インタフェースで送受信されたIPパケットのオクテット数や、各インタフェースの帯域使用率、各インタフェースで廃棄されたIPパケット数等の情報を収集する。トラヒック情報蓄積機構(106)は、このようにして収集されたトラヒックに関する情報を解析し、解析結果を日単位のトラヒック特性を示す日別トラヒック情報や、時間単位のトラヒック特性を示す時間別トラヒック情報として蓄積する。トラヒック情報解析機構(10

4)は、トラヒックに関する情報をもとに、現在のネットワーク内のトラヒック状況を判断したり、今後のネットワーク内のトラヒック状況を予見し、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)にポリシー情報を配布すべきか否かを判定し、ポリシー情報を配布すべきと判定した場合は、ポリシー制御部(102)にポリシー情報の配布要求を送信する(3b)。

【0019】ポリシー制御部(102)は、IPネットワークの使用状況に基づいて、ポリシー情報蓄積部(101)からポリシー情報を検索し(3a)、検索されたポリシー情報を、外部インタフェース(107)を介して、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に配布する(3c)。ルータ(200)や、帯域制御装置(300)、レイヤー2スイッチ(400)は、配布されたポリシー情報にもとづいてQoS (quality of service) やセキュリティの設定内容を変更する(3h)(3i)(3j)。このようにして、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に対し、IPネットワークの使用状況に応じたポリシー情報を配布し、QoS (quality of service) やセキュリティの設定内容を変更できる。

【0020】次に、ポリシー情報配布処理の動作を、シーケンス図を用いて説明する。図4は、ポリシー情報配布処理のシーケンス図である。ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、定期的にRMONで収集したトラヒックの統計情報や、MIB情報などの、IPネットワークのトラヒックに関する情報を、IPネットワーク制御装置(100)のトラヒック管理部(103)に送信する(4a)。

【0021】IPネットワーク制御装置(100)のトラヒック管理部(103)では、受信したIPネットワークのトラヒックに関する情報を解析し、ネットワーク内の通信品質やサービス品質を確保するために、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)のQoSやセキュリティの設定を変更するための、ポリシー情報を配布する必要があるか判定する。ここで、ポリシー情報を配布する必要があると判定された場合、ポリシー制御部(102)にポリシー情報の配布要求を送信する(4b)。ポリシー情報の配布要求を受信したポリシー制御部(102)では、どのような「条件」で、どのような「処理」を実施するポリシー情報がネットワークの使用状況に適しているか判定し、決定したポリシー情報をポリシー情報蓄積部(101)に検索要求を送信する(4c)。

【0022】ポリシー情報検索要求を受信したポリシー情報蓄積部(101)では、要求にあったポリシー情報を検索し、ポリシー制御部(102)に回答する(4d)。要求にあったポリシー情報の回答を受信したポリシー制御部(102)は、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)にポリシー情報を配布するために、TCPのコネクション確立要求をルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に送信する(4

e)。

【0023】ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)とポリシー制御部(102)間で、TCPのコネクションが確立した後(12f)、ポリシー制御部(102)はルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に、各装置のQoSやセキュリティの設定内容を変更するための権利を要求する(4g)。ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、ポリシー制御部(102)に装置のQoSやセキュリティの設定内容を変更するための権利を要求されたら、その権利をポリシー制御部(102)に付与する(4h)。

【0024】装置のQoSやセキュリティの設定内容を変更するための権利を付与されたポリシー制御部(102)は、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)にポリシー情報を配布する(4i)。要求にあったポリシー情報を受信したルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、ポリシー情報に従いQoSやセキュリティの設定内容を変更する。

【0025】以上により、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)のポリシー情報が設定される。

【0026】次に、ネットワーク管理者から、詳細まで定義されていないポリシー・サマリー情報が入力された場合の動作について説明する。図5に、ネットワーク管理者からポリシー・サマリー情報が入力された場合に、IPネットワーク制御装置がポリシー情報を配布する処理動作の一例のシーケンス図を示す。

【0027】ネットワーク管理者からのポリシー・サマリー情報を入力されたポリシー制御部(102)は、現状のネットワーク使用状況を知るために、トラヒック管理部(103)に、トラヒックに関する情報収集を要求する(5b)。トラヒックに関する情報収集を要求されたトラヒック管理部(103)は、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に、トラヒックに関するMIBを要求する(5c)。ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、トラヒック情報に関するMIB (management information base)を、IPネットワーク制御装置(100)のトラヒック管理部(103)に送信する(5d)。

【0028】IPネットワーク制御装置(100)のトラヒック管理部(103)では、受信したIPネットワークのトラヒックに関する情報を解析し、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)のQoSやセキュリティの設定を変更するために、ポリシー制御部(102)にポリシー情報の配布要求を送信する(5e)。ポリシー情報の配布要求を受信したポリシー制御部(102)では、どのような「条件」で、どのような「処理」を実施するポリシー情報がネットワークの使用状況に適しているか後述する処理を行って判定し、判定したポリシー情

報をポリシー情報蓄積部(101)に検索するよう要求する(5f)。

【0029】ポリシー情報検索要求を受信したポリシー情報蓄積部(101)では、要求にあったポリシー情報を検索し、ポリシー制御部(102)に回答する(5g)。このようにして最適なポリシー情報の回答を受信したポリシー制御部(102)は、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)にポリシー情報を配布するために、TCPのコネクション確立要求をルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に送信する(5h)。

【0030】ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)とポリシー制御部(102)間で、TCPのコネクションが確立した後(5i)、ポリシー制御部(102)はルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に、各装置のQoSやセキュリティの設定内容を変更するための権利を要求する(5j)。ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、ポリシー制御部(102)に装置のQoSやセキュリティの設定内容を変更するための権利を要求されたら、その権利をポリシー制御部(102)に付与する(5k)。

【0031】装置のQoSやセキュリティの設定内容を変更するための権利を付与されたポリシー制御部(102)は、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)にポリシー情報を配布する(5l)。ポリシー情報を受信したルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、ポリシー情報に従いQoSやセキュリティの設定内容を変更する。

【0032】以上により、ネットワーク管理者からポリシー・サマリー情報が入力された場合、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に最適なポリシー情報が設定される。

【0033】次に、ポリシー情報の配布の必要性を判定する処理について説明する。

【0034】図6はIPネットワーク制御機器(100)のトラヒック管理部(103)が、トラヒック情報を解析し、ポリシー情報の配布が必要であるか否かを判定する処理動作のフローチャートである。

【0035】IPネットワーク制御機器(100)のトラヒック管理部(103)が、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)からトラヒックに関する情報を収集すると(F601)、トラヒック情報処理機構(105)は、収集されたトラヒックに関する情報から、IPネットワークの使用状況に適したポリシー情報を策定するための評価パラメータ(例：パケット数、廃棄パケット数、RMON Trap通知回数等)を抽出し(F602)、トラヒック情報解析機構(104)は、抽出されたポリシー情報を策定するための評価データを、ファジー処理し、IPネットワークの使用状況を定量化し(F603)、IPネットワークの使用状況を示す数値から、現在のネッ

トワーク状況が良好か良好でないか判定し(F604)、良好であればフローの先頭に戻り、良好でなければポリシー制御部(102)に対し、ポリシー情報の配布を要求する(F605)。

【0036】図7、図8にIPネットワーク制御機器(100)のトラヒック管理部(103)が、抽出された評価パラメータをファジー処理し、IPネットワークの使用状況を定量化する手順の一例を示す。

【0037】図7と図8においては、理解を容易にするために例を簡略化して、インタフェースA(701)からルータ(200)に入り、インタフェースB(702)から送出されるトラヒック(703)を、ポリシー制御対象トラヒックとし、現在のネットワーク使用状況が良好か否か判定することとして説明する。

【0038】まず、ルータ(200)からトラヒックに関する情報を収集し(704)、ポリシー情報を策定するための評価パラメータを抽出する(705)。ここで、回線状態が「良好」であることファジー集合をMとし(801)、回線状態が「良好」であることを示すメンバシップ関数を $\mu(x)$ とする(802)。(ファジー集合とは、メンバシップ関数でその特性が定義されており、通常のクリスプ集合のように、ある要素の集合における度合いを0か1かの2値で判断するのではなく、0.0から1.0の連続した値で判断する理論である。)評価パラメータ(705)の各要素(送受信パケット数やパケット廃棄数を示す要素 x_1, x_2, x_3, x_4)のファジー集合Mにおける度合いをメンバシップ関数より求めると、右下がり型のメンバシップ関数となる(803)。こうして求めた評価パラメータの各要素のファジー集合Mにおける度合いから、IPネットワークの使用状況が定量化できる(804)。

【0039】図9は、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)からのトラヒックに関する情報にもとづき、IPネットワーク制御装置(100)がポリシー情報を、最適な契機に配布する処理動作の一例のシーケンス図を示している。

【0040】ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、定期的にRMONで収集したトラヒックの統計情報や、MIB情報などの、IPネットワークのトラヒックに関する情報を、IPネットワーク制御装置(100)のトラヒック管理部(103)に送信する(9a)。

【0041】IPネットワーク制御装置(100)のトラヒック管理部(103)では、受信したIPネットワークのトラヒックに関する情報を解析し、ネットワーク内の通信品質やサービス品質を確保するために、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)のQoSやセキュリティの設定を変更するための、ポリシー情報を配布する必要があるか判定する。ここで、ポリシー情報を、IPネットワークの使用状況が良好でなく

なると予見される、x分後に配布する必要があると判定された場合、x分のタイマー設定を行い、タイムアウト後、ポリシー制御部(102)にポリシー情報の配布要求を送信する(9b)。

【0042】ポリシー情報の配布要求を受信したポリシー制御部(102)では、どのような「条件」で、どのような「処理」を実施するポリシー情報がネットワークの使用状況に適しているか判定し、決定したポリシー情報をポリシー情報蓄積部(101)に検索要求を送信する(9c)。

10 ポリシー情報検索要求を受信したポリシー情報蓄積部(101)では、要求にあったポリシー情報を検索し、ポリシー制御部(102)に回答する(9d)。

【0043】最適なポリシー情報の回答を受信したポリシー制御部(102)は、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)にポリシー情報を配布するために、TCPのコネクション確立要求をルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に送信する(9e)。

20 【0044】ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)とポリシー制御部(102)間で、TCPのコネクションが確立した後(9f)、ポリシー制御部(102)はルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に、各装置のQoSやセキュリティの設定内容を変更するための権利を要求する(9g)。ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、ポリシー制御部(102)に装置のQoSやセキュリティの設定内容を変更するための権利を要求されたら、その権利をポリシー制御部(102)に付与する(9h)。

30 【0045】装置のQoSやセキュリティの設定内容を変更するための権利を付与されたポリシー制御部(102)は、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)に最適なポリシー情報を配布する(9i)。最適なポリシー情報を受信したルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)は、ポリシー情報に従いQoSやセキュリティの設定内容を変更する。

【0046】以上により、ルータ(200)や、帯域制御装置(300)や、レイヤー2スイッチ(400)のポリシー情報が設定される。

40 【0047】以上説明した通り、本発明によれば、ポリシーを策定する際に、RMONプローブやMIB等で収集されたパケット数や帯域使用率等のトラヒック情報を、ネットワーク管理者が任意に決めるようなしきい値を用いて「何Kbps以上はトラヒックが多い」「何%以下は帯域が不足」と判断するのではなく、IPネットワーク機器から収集した、トラヒックに関する情報から評価パラメータを抽出し、抽出した評価パラメータからIPネットワークの使用状況をメンバシップ関数を用いて定量化し、蓄積されているポリシー情報から、ネットワークの使用状況に最適なポリシー情報を検索し、最適

な契機に配布する制御にファジー制御を用いることで、IPネットワークの使用状況に応じたポリシー制御を実施することが可能となる。

【0048】

【発明の効果】本発明によれば、IPネットワークの使用状況に応じた最適なポリシー制御を実施することが可能となる。

【図面の簡単な説明】

【図1】本発明を適用したIPネットワークの構成の概要について示した図である。

【図2】IPネットワーク制御装置の構成を示す図である。

【図3】ポリシー情報配布処理の概要を示す図である。

【図4】IPネットワーク制御装置におけるポリシー情報配布処理のシーケンス図である。

【図5】ネットワーク管理者からポリシー・サマリー情報が入力された場合のポリシー情報配布処理を示すシー

ケンス図である。

【図6】トラヒック管理部におけるポリシー情報配布可否を判定する処理を説明するフローチャートである。

【図7】トラヒック管理部におけるIPネットワークの使用状況を定量化する手順を説明する図である。

【図8】トラヒック管理部におけるIPネットワークの使用状況を定量化する手順を説明する図である。

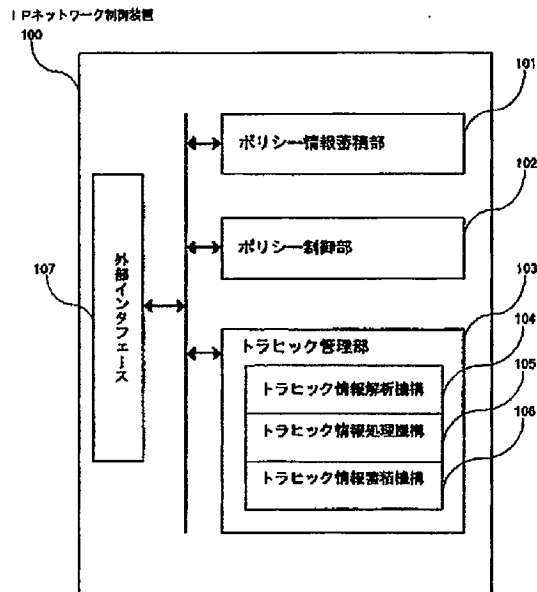
【図9】IPネットワーク制御装置のポリシー情報配布処理を説明するシーケンス図である。

10 【符号の説明】

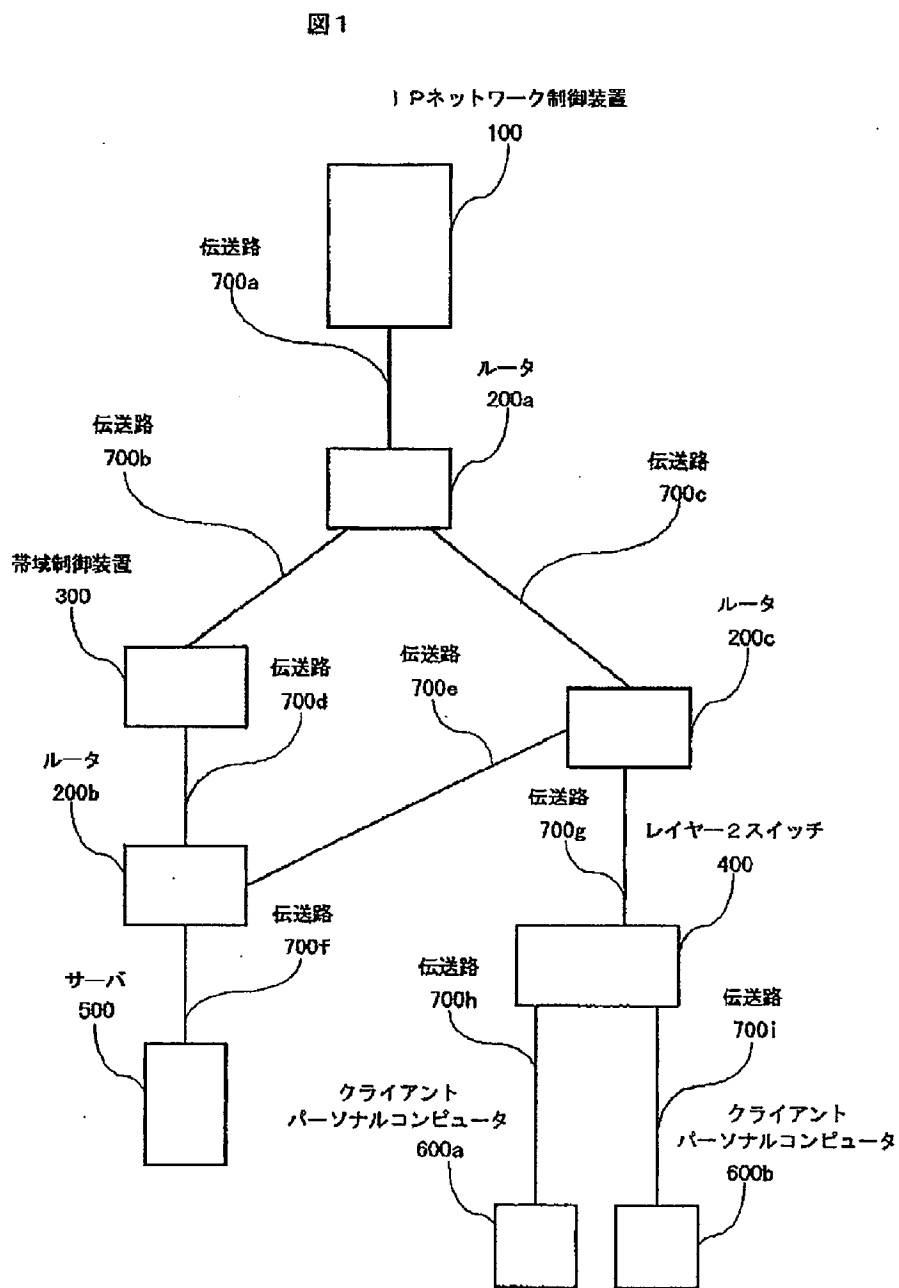
100…IPネットワーク制御装置、101…ポリシー情報蓄積4…トラヒック情報解析機構、105…トラヒック情報処理機構、106…トラヒック情報蓄積機構、107…外部インタフェース、200a、200b、200c…ルータ、300…帯域制御装置、400…レイヤー2スイッチ、500…サーバ、600a、600b…クライアントパーソナルコンピュータ、700a～700i…伝走路。

【図2】

図2

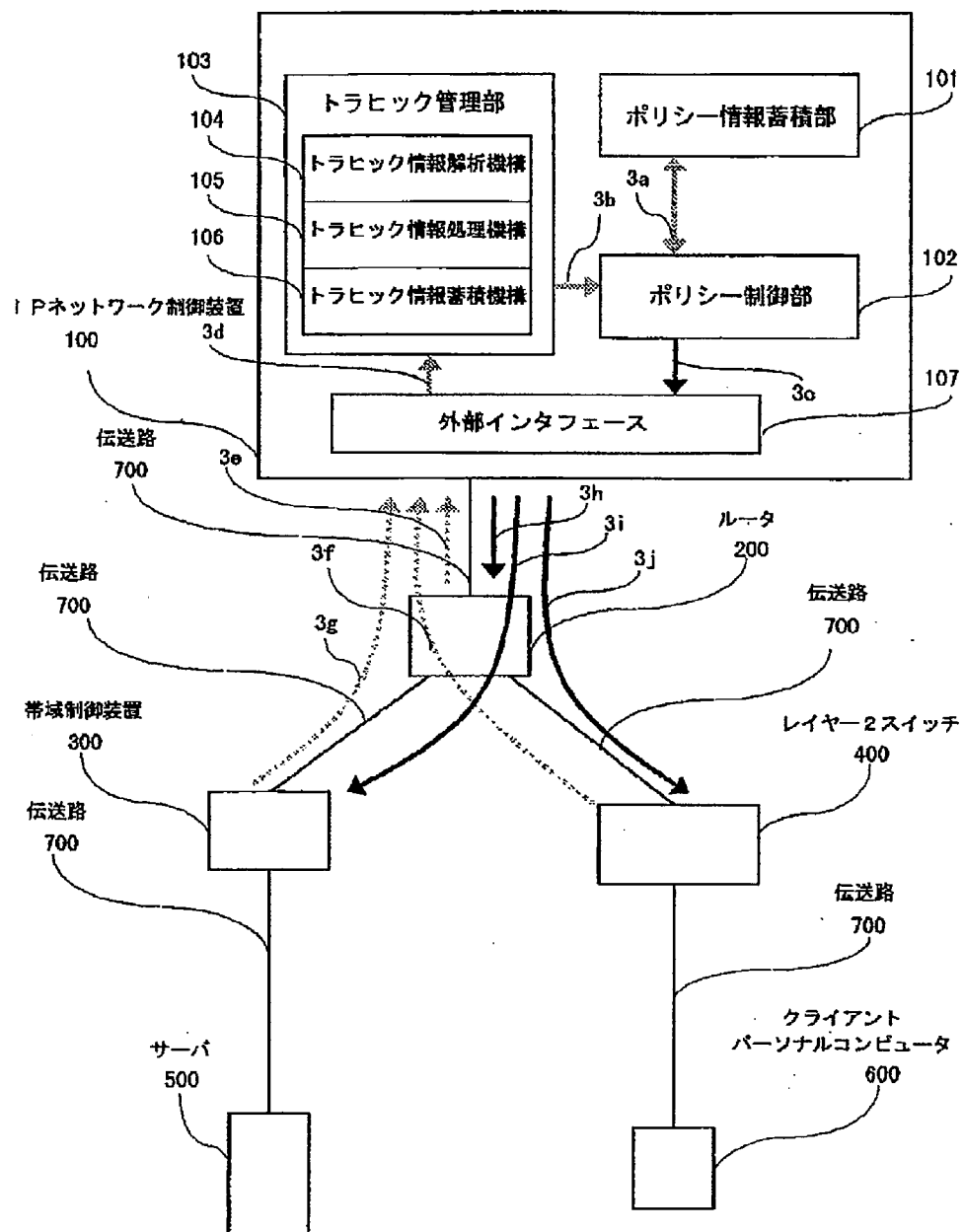


【図 1】



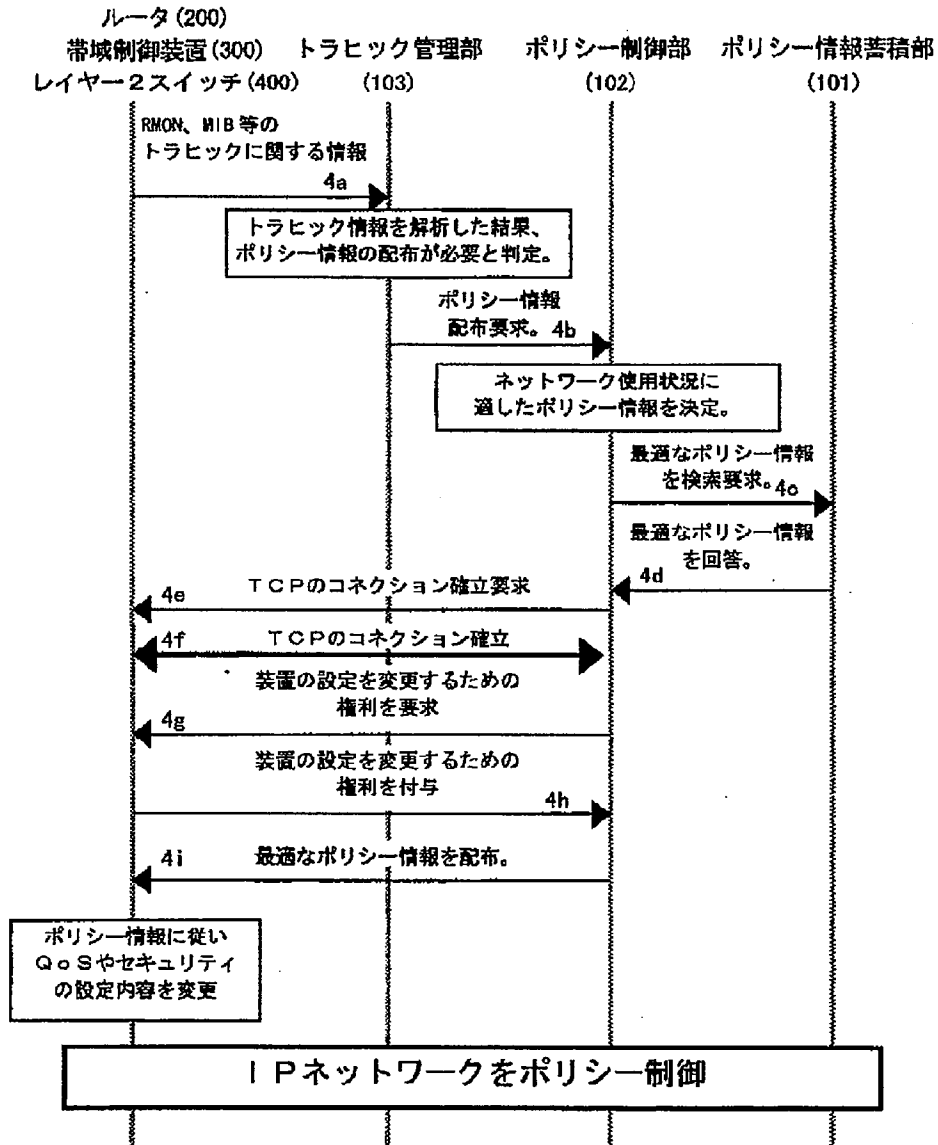
【図 3】

図 3



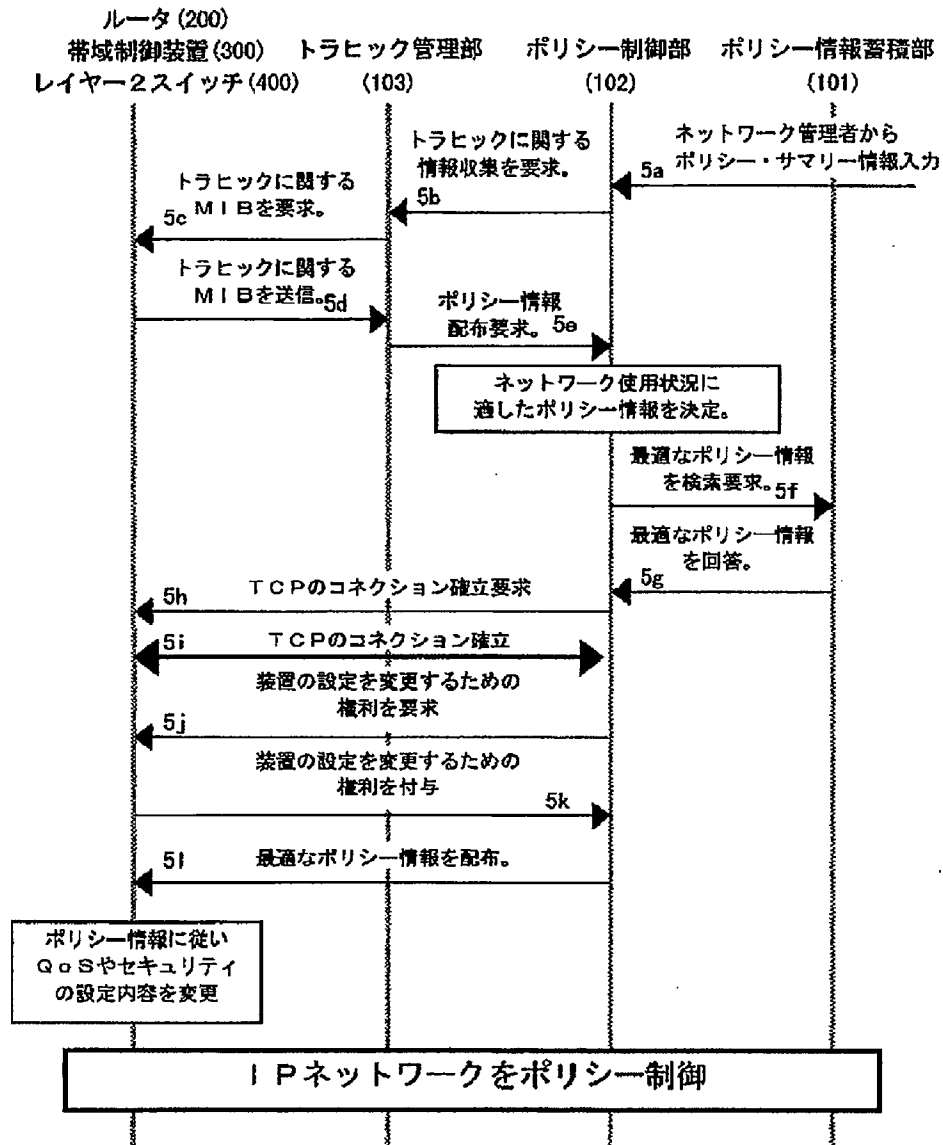
【図 4】

図 4



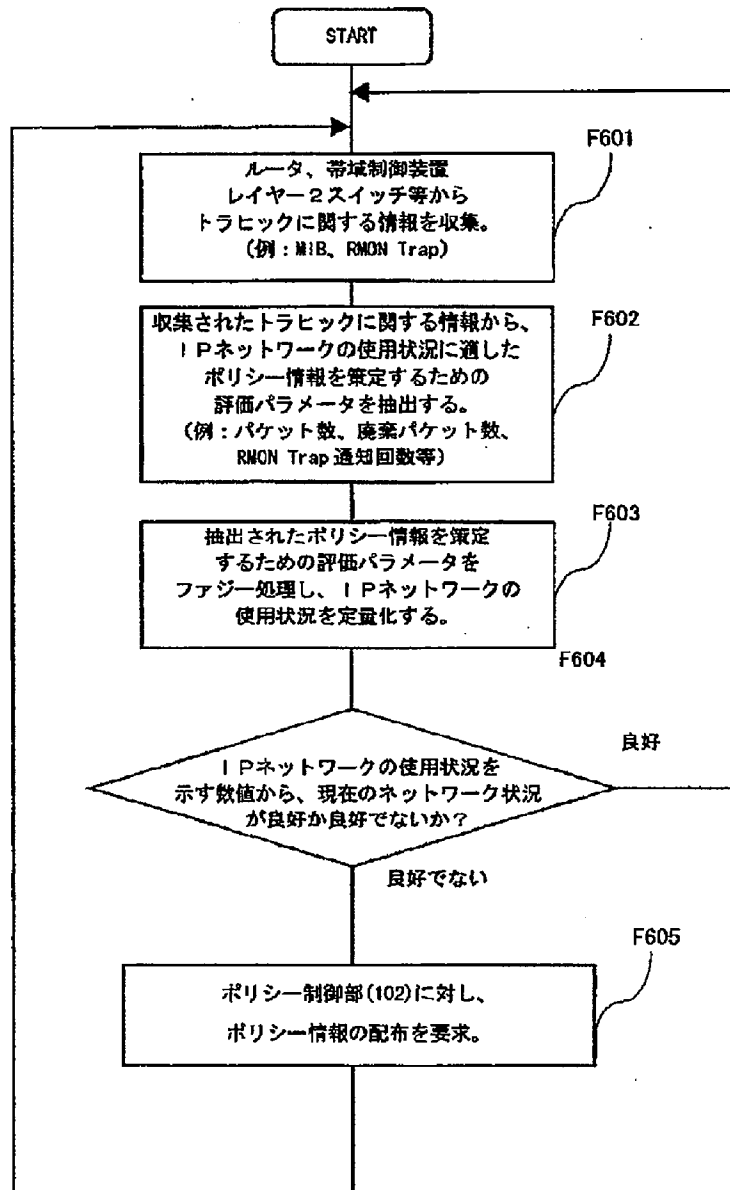
【図 5】

図 5



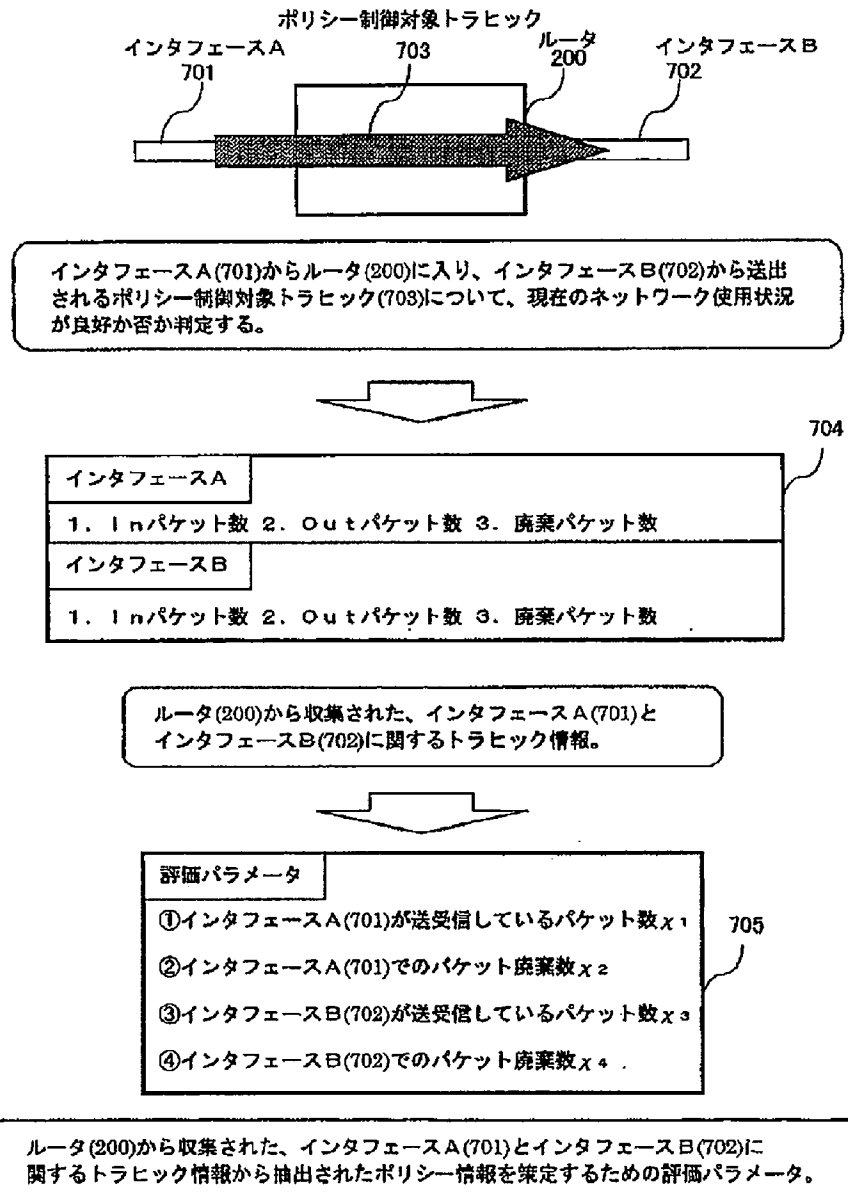
【図 6】

図 6



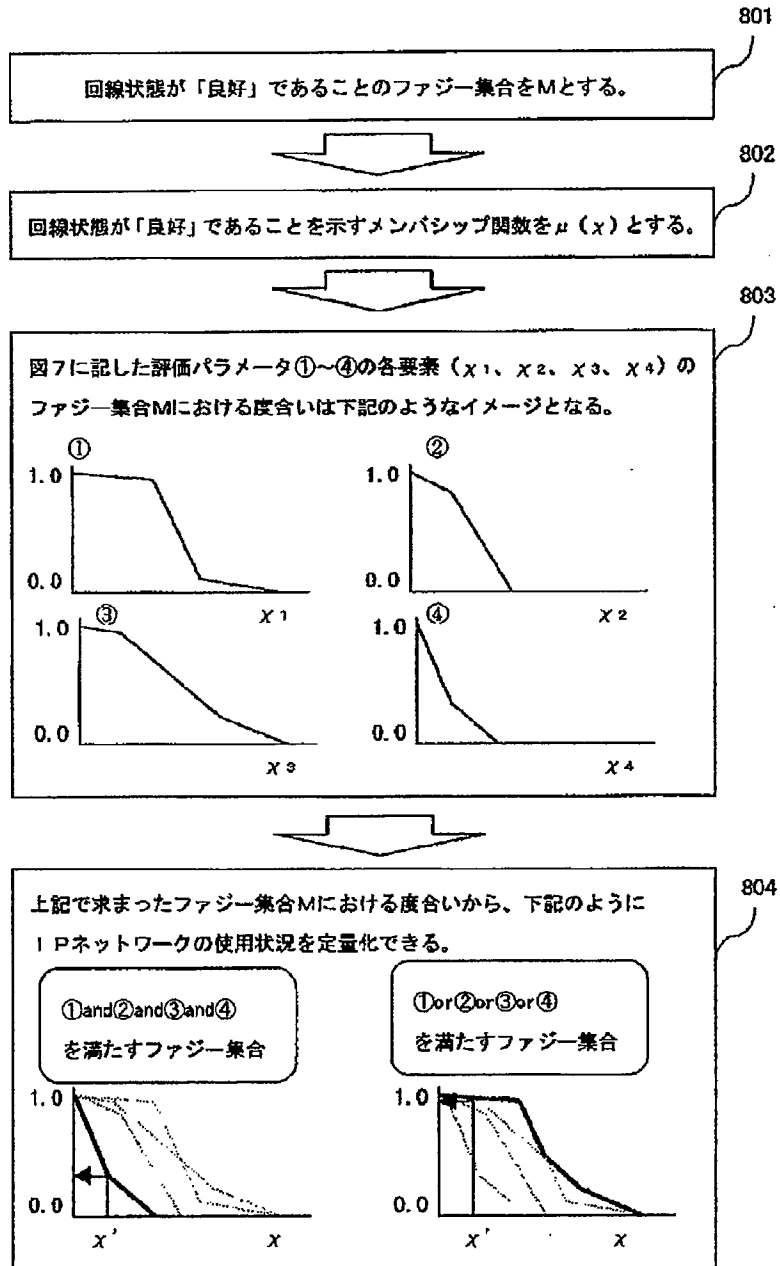
【図 7】

図 7



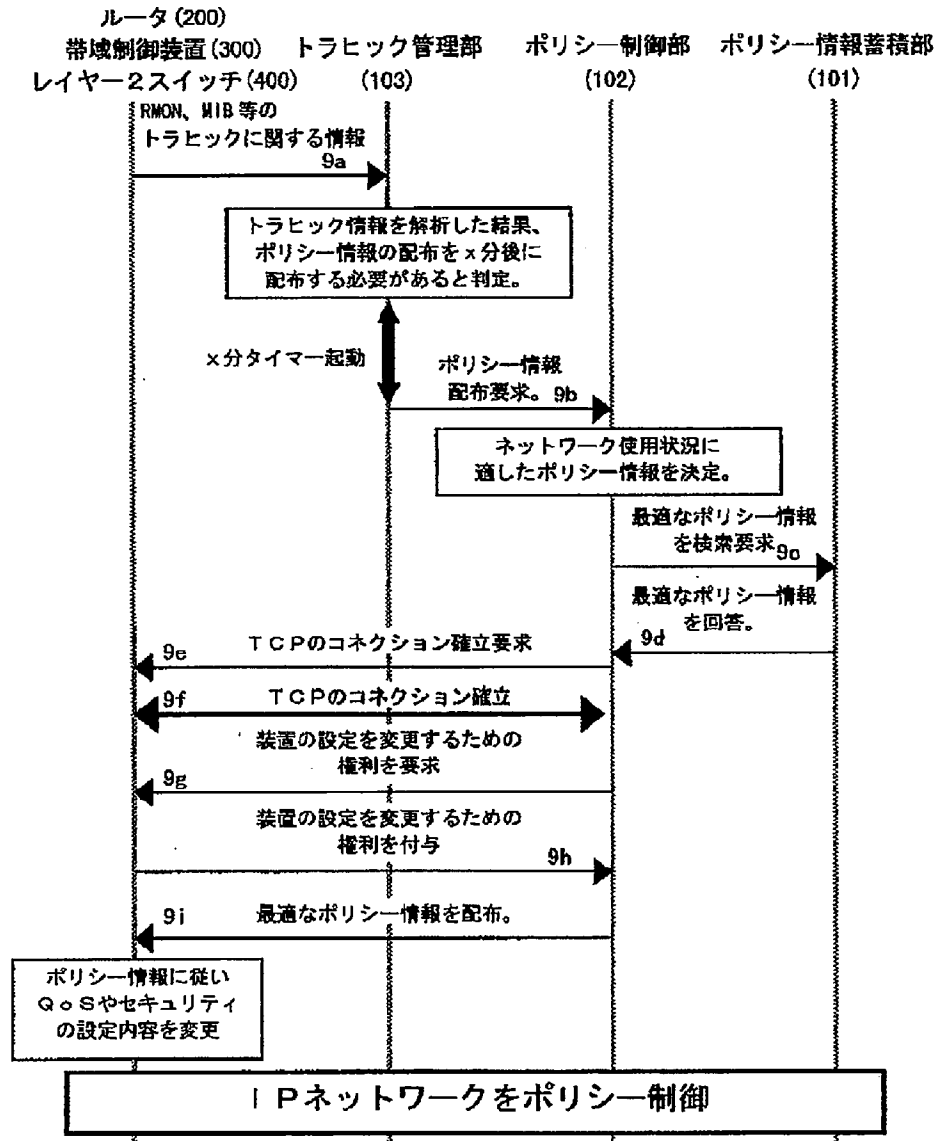
【図 8】

図 8



【図 9】

図 9



フロントページの続き

(72) 発明者 平良 正憲
 神奈川県川崎市幸区鹿島田890番地 株式
 会社日立製作所社会・ネットワークシステ
 ム事業部内

F ターム(参考) 5K030 GA11 HA08 HC01 HD03 JA10
 JL07 KA01 KA05 KA07 KX30
 LB05 MA01 MB09 MC09